NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

$1 million fire at N.D. tire, oil facility. A February 17 multi-alarm fire at Vining Oil in Jamestown, North Dakota, caused an estimated $1 million in damage and losses. The mid-morning fire completely engulfed a warehouse-type structure that housed "several" 55-gallon barrels of oil, some 600-700 medium truck tires, and two tractors. The fire completely destroyed the building and caused damage to adjacent businesses. Some nearby hotels had to evacuate guests due to the thick black smoke from the fire that hovered over the area. Fire officials are still investigating the cause of the fire. Source: http://www.tirereview.com/Article/97221/1_million_fire_at_nd_tire_oil_facility.aspx

Regional

(Minnesota) **Water filtration plant in Columbia Heights evacuated after chemicals mixed; no injuries.** A water treatment facility in Columbia Heights, Minnesota, was evacuated after two chemicals were accidentally mixed together and caused a reaction February 14. The assistant fire chief said workers notified the Columbia Heights Fire Department that hydrochloric acid and caustic soda had been combined at the plant. When mixed, the two chemicals cause excessive heat. The heat caused the building's sprinkler system to go off. All employees were immediately evacuated. The assistant fire chief did not know how the chemicals were incorrectly mixed. The plant is the City of Minneapolis' water filtration plant. Minneapolis officials said drinking water was never at risk of contamination and that the city's tap water is safe to drink. Source: http://www.therepublic.com/view/story/09763953dc2c4654a87474294e4a46d4/MN--Water-Treatment-Evacuation/

National

U.S. opening up airspace to use of drones. Legislation passed by U.S. Congress the week of February 13 gives the Federal Aviation Administration (FAA) until September 30, 2015, to open the nation's skies to drones. The first step comes in 90 days when police, firefighters, and other civilian first-response agencies can start flying UAVs weighing no more than 4.4 pounds, provided they meet still-to-be-determined requirements, such as having an operator on the ground within line-of-sight of the drone and flying it at least 400 feet above ground. Currently, UAVs can only fly in restricted airspace zones controlled by the U.S. military. By May 2013, the next class of drones, those weighing less than 55 pounds, can fly the nation's skies, according to provisions of the FAA bill passed by Congress and signed by the U.S. President. Rules about where and when drones can fly and who can operate them are still under development. And there are still technical hurdles, such as setting up the bandwidth for secure UAV radio communications and refining collision avoidance systems, said the NASA program manager of the Dryden Flight Research Center at Edwards, California. Source: http://www.msnbc.msn.com/id/46499162/ns/technology_and_science-science/#.T0emfHn_QpK

GPS jammers and spoofers threaten infrastructure, say researchers. During the Global Navigation Satellite System (GNSS) Vulnerability 2012 event at Great Britain's National Physical Laboratory February 22, experts discussed the threat posed by a growing number of GPS jamming and spoofing devices. The increasing popularity of jammers is troubling, according to the conference organizer, because even low-power GPS jammers pose a significant threat to cell phone systems, parts of the electrical grid, and drivers. Since cell phone towers and some electrical grid systems use GPS signals for time-keeping, jamming can throw them off and cause outages. "We're seeing a large number of low power devices which plug into power sockets in a car," the conference organizer said. "These devices take out the GPS tracker in the vehicle, but they also create a 'bubble' of interference, sometimes out to up to 100 yards. They are illegal, so their quality control is generally not good." One presenter at the conference, an assistant professor at the University of Texas, presented findings on the impact of spoofing and jamming on cell phones. The professor, who claims his lab possesses the most powerful civilian-owned GPS spoofer, said that in U.S. tests, his team succeeded in interfering with timing devices used in cellular network towers, breaking down synchronization between cells, and preventing calls from being handed off from one cellular station to another. "So far, no credible high profile attack has been recorded," he said, "but we are seeing evidence of basic spoofing, likely carried out by rogue individuals or small groups." Small short-range jammers have created isolated problems in the United States. In late 2009, a single truck using a GPS jammer caused problems at the Newark Liberty International Airport in New Jersey as it interfered with a navigation aid every time the truck passed on the New Jersey Turnpike. Truck drivers and other drivers who want to conceal their movements from tracking devices sometimes use basic GPS jammers embedded in their vehicles. Source: http://arstechnica.com/business/news/2012/02/uk-research-measures-growing-gps-jamming-threat.ars

INTERNATIONAL

Inspections reveal serious flaws at 11 Bulgarian dams. The ongoing inspection of the condition of dams located all over Bulgaria has so far identified serious problems at 11 facilities of a total of 140 checked, according to the minister of economy, energy and tourism. After a meeting February 15, he explained the problematic dams were located in five districts — one in Kardzhali, one in Smolyan, two in Montana, three in Pazardzhik, and three in Sliven. Like the Elena dam, which was subjected to a controlled draining February 13 over a risk of failure, the majority of the faulty reservoirs have non-functioning spillways and release gates, the CEO of the national power grid operator, NEK, concluded. He warned the release gates of the dams needed urgent repairs and the facilities had to be equipped with emergency gates. Source: http://www.novinite.com/view_news.php?id=136693

Monsanto guilty of chemical poisoning in France. A French court February 13 declared U.S. biotech giant Monsanto guilty of chemical poisoning of a French farmer, a judgment that could lend weight to other health claims against pesticides. In the first such case heard in France, a grain grower said he suffered neurological problems including memory loss, headaches, and stammering after inhaling Lasso weedkiller in 2004. He blames the agri-business giant for not providing adequate warnings on the product label. The court in Lyon sought an expert opinion

of losses to establish damages. Previous health claims from farmers have foundered because of the difficulty of establishing clear links between illnesses and exposure to pesticides. The grain grower joined with other farmers suffering from illness to set up an association last year. The agricultural branch of the French social security system said since 1996, it has gathered about 200 reports a year of farmers' claiming they were sickened by pesticides. But only 47 cases in the past 10 years have been recognized as due to pesticides. Source: http://www.reuters.com/article/2012/02/13/france-pesticides-monsanto-idUSL5E8DD5UG20120213

Banking and Finance Industry

Record $6 trillion of fake U.S. bonds seized. Italian anti-mafia prosecutors said they seized a record $6 trillion of allegedly fake U.S. Treasury bonds, an amount that is almost half of the U.S.'s public debt, Bloomberg reported February 17. The bonds were found hidden in makeshift compartments of three safety deposit boxes in Zurich, Switzerland, prosecutors from the southern city of Potenza said in an e-mailed statement. The Italian authorities arrested eight people in connection with the probe. The U.S. embassy in Rome examined the securities dated 1934, which had a nominal value of $1 billion a piece, they said in the statement. The financial fraud uncovered by the Italian prosecutors in Potenza includes two checks issued through HSBC Holdings Plc in London for 205,000 pounds ($325,000), checks that were not backed by available funds, the prosecutors said. As part of the probe, fake bonds for $2 billion were also seized in Rome. The individuals involved were planning to buy plutonium from Nigerian sources, according to phone conversations monitored by the police. The fraud posed "severe threats" to international financial stability, the prosecutors said in the statement. Phony U.S. securities have been seized in Italy before and there were at least three cases in 2009. Italian police seized phony U.S. Treasury bonds with a face value of $116 billion in August of 2009 and $134 billion of similar securities in June of that year. Source: http://www.bloomberg.com/news/2012-02-17/italy-police-seize-6-trillion-of-fake-u-s-treasury-bonds-in-switzerland.html

FTC action leads to ban on alleged mortgage relief scammers who harmed thousands of consumers. At the request of the Federal Trade Commission (FTC), a U.S. district court February 14 put the mortgage relief business permanently off limits to marketers who allegedly charged thousands of consumers up to $2,600 each, based on bogus promises to provide loan modifications that would make mortgages more affordable. According to the FTC, the scheme caused consumer losses of nearly $19 million. All but two of the defendants settled with the agency, while the two other corporate defendants received default judgments. The FTC alleged the defendants used direct mail, the Internet, and telemarketing to target homeowners. The defendants typically asked for half of the fee up-front, falsely claiming a success rate of up to 100 percent, according to the complaint. They deceptively claimed they could prevent foreclosure, that they were affiliated with or approved by consumers' lenders, and that they would refund consumers' money if they failed to deliver promised services, according to the FTC. They told consumers not to contact lenders and to stop making mortgage payments, claiming that falling behind on payments would demonstrate hardship, the FTC alleged. The

complaint charged U.S. Mortgage Funding, Inc., Debt Remedy Partners Inc., Lower My Debts.com LLC, and four individuals with violating the FTC Act and the FTC's Telemarketing Sales Rule. The court orders ban all the defendants from providing mortgage and debt relief services and telemarketing. Source: http://www.ftc.gov/opa/2012/02/usmortgage.shtm

Chemical and Hazardous Materials Sector

NRC examines U.S. response to Fukushima. February 21, the Nuclear Regulatory Commission (NRC) released about 3,000 pages of transcripts of conversations recorded in its operations center after the Fukushima Daiichi nuclear disaster, conversations that underscore the difficulty the agency had in responding to the crisis unfolding halfway around the world. The transcripts, released in response to Freedom of Information Act requests, show agency officials struggling to get information about the disaster and trying to ascertain its potential impact on U.S. citizens in Japan, on potential fallout victims in the United States, and on operators of U.S. nuclear reactors of similar design. The transcripts are of conversations and phone calls at the NRC's operations center in Rockville, Maryland. Agency officials said the Fukushima experience demonstrated the "significant limitation" the United States had on getting data about an incident "halfway around the world." Officials also said previous exercises in the command center had not fully prepared them for what turned out to be a months-long event that required teams of people working round-the-clock for months. They said they did not communicate as fully as they should have with state officials seeking information about the potential for fallout and the safety of their own nuclear plants. Source: http://www.krcrtv.com/news/30511475/detail.html

Dust from industrial-scale processing of nanomaterials carries high explosion risk. With expanded industrial-scale production of nanomaterials fast approaching, scientists are reporting indications that dust generated during processing of nanomaterials may explode more easily than dust from wheat flour, cornstarch, and most other common dust explosion hazards, according to a February 15 release from the American Chemical Society (ACS). Their article in ACS' journal Industrial & Engineering Chemistry Research indicates that nanomaterial dust could explode due to a spark with only 1/30th the energy needed to ignite sugar dust — the cause of the 2008 Portwentworth, Georgia, explosion that killed 13 people, injured 42 people, and destroyed a factory. After reviewing results of studies that exist on the topic, the researchers concluded that the energy needed to ignite nanomaterials made of metals, such as aluminum, is less than 1 mJ, which is less than 1/30th the energy required to ignite sugar dust or less than 1/60th the energy required to set wheat dust aflame. Flocking is often made with a process that generates static electricity, which could set off an explosion of flocculent dust, they point out. And the addition of a flammable gas or vapor to a dust as a hybrid mixture increases the chance that the dust will explode. The researchers warn that precautions should be taken to prevent these materials from exposure to sparks, collisions, or friction, which could fuel an explosion. Source: http://portal.acs.org/portal/acs/corg/content?_nfpb=true&_pageLabel=PP_ARTICLEMAIN&node_id=223&content_id=CNBP_029293&use_sec=true&sec_url_var=region1&__uuid=912905f8-dcbd-4315-8799-b3fa9e5e6cec

EPA sets new rules for emissions from PVC production. The Environmental Protection Agency (EPA) February 14 set stringent emissions limits for industrial plants that manufacture polyvinyl chloride, a ubiquitous plastic commonly known as PVC. The new rule comes two years after a settlement between three activist groups and the EPA. The Sierra Club and two community groups in Louisiana filed a lawsuit in 2008 to force the agency to establish limits for several harmful pollutants at the nation's 17 vinyl-producing plants, including four in Texas. The rule sets limits for three air toxics — vinyl chloride, chlorinated di-benzo dioxins and furans, and hydrogen chloride. The previous rule only covered vinyl chloride, a known carcinogen. The EPA estimates the tougher standard will reduce emissions by 262 tons annually, with the cost of compliance at $4 million a year after an initial capital investment of $18 million. The Vinyl Institute, an industry group based in Virginia said the rule's economic impact could be as high as $100 million, based on the EPA's earlier proposal. Source: http://www.chron.com/news/houston-texas/article/EPA-sets-new-rules-for-emissions-from-PVC-3324417.php

Committee leaders express concern over EPA policy that could compromise chemical facility security. U.S. House Energy and Commerce Committee leaders sent a letter February 10 to the Environmental Protection Agency (EPA) administrator expressing concern over a recent announcement that they claimed could compromise sensitive data and make U.S. chemical manufacturing facilities more susceptible to terrorist attacks. They voiced strong opposition to the EPA's decision to re-establish Internet access to manufacturers' non-Off-site Consequence Analysis sections of the Risk Management Plan database, sections that contain lists of covered chemicals used, preventative measures, and the location in a plant where those chemicals are used. The leaders asked the administrator to reverse the decision. In the letter, they argued publishing the data could provide "a virtual terrorist roadmap into a chemical facility." They added: "This is why EPA decided to remove all Risk Management Plan data from the Agency website in the fall of 2001." Source: http://energycommerce.house.gov/news/PRArticle.aspx?NewsID=9292

Industry progressing in voluntary effort to reduce toxic chemicals. The U.S. Environmental Protection Agency (EPA) released February 10 interim results of a voluntary effort by eight chemical manufacturers to reduce emissions and use of long-chain perfluorinated chemicals (LCPFCs), including perfluorooctanoic acid (PFOA). Used in hundreds of manufacturing and industrial applications, LCPFCs are toxic, persistent in the environment worldwide, and can accumulate in people. The agency's 2010/15 PFOA Stewardship Program was established in 2006 in partnership with eight companies. The program set a goal of reducing facility emissions and product content of PFOA and related chemicals on a global basis by 95 percent, no later than 2010, and to work toward eliminating emissions and product content by 2015. Daikin America, Inc., DuPont, 3M/Dyneon, and Solvay Solexis met the program's intermediate goal of a 95 percent reduction in emissions and product content by 2010, the EPA said. It noted 150 replacement chemicals have been developed. The eight manufacturers informed the EPA they are on track to phase out LCPFCs by the end of 2015. Source:

http://news.thomasnet.com/companystory/Voluntary-Effort-Makes-Progress-in-reducing-LCPFCs-PFOA-609677

EPA moves to prevent fuel spills on farms. The Environmental Protection Agency (EPA) is requiring farmers with 10,000 gallons of fuel storage or more to come up with engineer-certified fuel spill containment facilities, the Billings Gazette reported February 10. Smaller farms with storage below the 10,000 mark but more than 1,320 gallons have to complete a self-designed plan for containing fuel spills. Farm fuel spills have been only softly regulated by the EPA, but the agency is bringing more focus on spills out of concern for water quality and levying fines of more than $1,000 for major noncompliance. The Natural Resources and Conservation Service (NRCS) began offering Montana farmers help with the plan design and construction costs. The NRCS is getting involved because it would like plans that not only address risks to rivers and streams, but also groundwater.Source: http://billingsgazette.com/news/state-and-regional/montana/epa-moves-to-prevent-fuel-spills-on-farms/article_0325148a-cd86-57b8-9bff-c41fec1102bc.html

Commercial Facilities

Nothing Significant to Report

Communications Sector

Smartphone security gap exposes location, texts, email, expert says. A former McAfee cybersecurity researcher has used a previously unknown hole in smartphone browsers to deliver an existing piece of China-based malware that can commandeer the device, record its calls, pinpoint its location, and access user texts and e-mails. He conducted the experiment on a phone running Google's Android operating system, although he said Apple's iPhones are equally vulnerable. He is scheduled to demonstrate his findings February 29 at the RSA conference in San Francisco. The researcher said he and his team commandeered an existing piece of malware called Nickispy, a remote access tool identified in 2011 by anti-virus firms as a trojan. The malware was disguised as a Google+ app that users could download. However, Google quickly removed it from its Android Market app store, which meant few users were hit. The researcher and his team reversed engineered the malware and took control of it. He then conducted an experiment in which malware was delivered through a "spear phishing" attack — in this case, a text message from what looks like a mobile phone carrier. He said he exploited a zero-day vulnerability in smartphone browsers to secretly install the malware. "The minute you go the site, it will download a real-life Chinese remote access tool to your phone," he said. "The user will not see anything. Once the app is installed, we'll be intercepting voice calls. The microphone activates the moment you start dialing." The malware also intercepts texts and e-mails and tracks the phone's location, he said. In theory, it could be used to infiltrate a corporate network with which the phone connects. There is no security software that would thwart it, he said. Source: http://www.latimes.com/business/technology/la-fi-tn-cyber-security-crowdstrike-20120223,0,4645028.story

Anonymous vows to shut down the Internet. Anonymous has threatened to launch Operation Global Blackout (OpGlobalBlackout), which calls for supporters to download a denial-of-service launching tool, called "Ramp," which will flood the 13 root Domain Name Servers (DNS) of the Internet with more requests than they can process, SecurityNewsDaily reported February 16. February 12, an announcement appeared on the file-hosting site Pastebin declaring March 31 as the day "anonymous will shut the Internet down." The manager for Root Zone Services at the Internet Corporation for Assigned Names and Numbers said, "There are not 13 root servers. There are many hundreds of root servers at over 130 physical locations in many different countries." This discrepancy is critical, said a consultant from Errata Security. "The Anonymous hackers can certain(ly) cause local pockets of disruption, but these disruptions are going to be localized to networks where their attack machines are located," he wrote. "They might affect a few of the root DNS servers, but it's unlikely they could take all of them down, at least for any period of time. On the day of their planned Global Blackout, it's doubtful many people would notice." Source: http://www.msnbc.msn.com/id/46420147/ns/technology_and_science-security/#.Tz57CYGLcdU

University of Minnesota researchers discover that cell phone hackers can track your physical location without your knowledge. Cellular networks leak the locations of cell phone users, allowing a third party to easily track the location of the cell phone user without the user's knowledge, according a February 16 press release announcing the findings of new research by computer scientists in the University of Minnesota's College of Science and Engineering. Using an inexpensive phone and open source software, the researchers were able to track the location of cell phone users without their knowledge on the Global System for Mobile Communications (GSM) network, the predominant worldwide network. In a field test, the research group was able to track the location of a test subject within a 10-block area as the subject traveled across an area of Minneapolis at a walking pace. The researchers used readily available equipment and no direct help from the service provider. The researchers have contacted AT&T and Nokia with low-cost techniques that could be implemented without changing the hardware, and are in the process of drafting responsible disclosure statements for cellular service providers. Source: http://www1.umn.edu/news/news-releases/2012/UR_CONTENT_374462.html

(Kansas) **Copper thief pleads guilty to damaging utility.** A Kansas copper thief is looking at a possible 20 years in prison for pulling down power poles to get at the wiring, the Kansas City star reported February 13. His action also caused a southeastern Kansas radio station to go off the air for several hours. He was finally stopped by an armed property owner who caught him trying to steal a copper coupling from his propane tank, prosecutors said. He pleaded guilty February 13 to one count of damaging an energy facility. A second charge of obstructing the national Emergency Alert System by putting the radio station out of commission was dropped. The man stole copper wire September 7 by pulling down an electrical pole belonging to the Heartland Rural Electric Company. That caused a second pole also to fall. And that affected radio station KKOW in Pittsburg, Kansas, whose transmission tower was at the site. Source: http://www.kansascity.com/2012/02/13/3427390/copper-thief-pleads-guilty-to.html

Critical Manufacturing

NHTSA recall notice - Kawasaki Ninja ZX battery regulator. Kawasaki announced February 24 the recall of 20,544 model year 2008-2011 Ninja ZX-10R and 2009-2012 Ninja ZX-6R motorcycles manufactured from December 14, 2007 through July 26, 2011. Due to a manufacturing error, the regulator/rectifier may insufficiently charge the battery. If the battery discharges, the motorcycle may stall without warning, increasing the risk of a crash. Kawasaki will notify owners, and dealers will replace the voltage regulator. The safety recall is expected to begin on or about February 27. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V064000&summary=true&prod_id=1433770&PrintVersion=YES

NHTSA recall notice - Porsche Cayenne headlights. Porsche announced February 24 the recall of 20,278 model year 2011-2012 Cayenne, Cayenne S, Cayenne S Hybrid, and Cayenne Turbo vehicles manufactured from March 8, 2010 through January 31, 2012 because the headlamps may come loose and detach from the fender. A detached headlight could lead to loss of visibility and an increased risk of a crash. Porsche will notify owners, and dealers will replace the headlamp locking assemblies. The safety recall was expected to begin on February 23. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V065000&summary=true&prod_id=1433775&PrintVersion=YES

Meijer recalls Touch Point fan heaters due to fire, shock hazards. The U.S. Consumer Product Safety Commission, in cooperation with Meijer Inc., February 22 announced a voluntary recall of about 6,102 Touch Point Forced Air Heaters. Consumers should stop using recalled products immediately unless otherwise instructed. Exposed and unshielded electrical components can cause the heater to overheat and melt, posing fire and shock hazards. Meijer received one report of a unit's base burning, melting, and damaging the carpet beneath it. No injuries have been reported. The heaters were sold in Meijer stores in Illinois, Indiana, Kentucky, Michigan, and Ohio. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12115.html

Nissan recalls 250,000 cars worldwide. Nissan Motor Company said February 23 it was recalling about 250,000 vehicles globally, to correct a flaw with fuel sensors that can result in leaks. The recall covers seven different models equipped with "direct injection type engine," including the Nissan Serena, Juke, Patrol, Tiida, and Micra. The Infiniti QX56 SUV and M56 luxury sedan were also named in the recall. Nissan said it was not aware of any accidents or injuries related to the flaw. The company said it found the "fuel rail pressure sensor's tension may decrease over time." As a result, fuel leakage may occur in a worst-case scenario. Source: http://www.q13fox.com/news/kcpq-nissan-recalls-250000-cars-worldwide-20120223,0,1467035.story?track=rss

NHTSA recall notice - Navistar IC Bus and International models traction relay valves. Navistar announced February 16 that it recalled 18,959 model year 2012-2013 IC Bus HC and International 9400, and certain model year 2011-2013 International Durastar, Payster,

Workstar, Transtar, Lonestar, Prostar, 9200, and 9800, and certain model year 2013 International 9900 vehicles manufactured from December 2, 2010, through January 26, 2012 and equipped with Bendix ATR-6 traction relay valves. In extremely cold conditions these valves may develop internal leakage. Leakage can lead to air pressure being delivered to affected primary or secondary brakes, causing continuous brake application. Unexpected continuous brake application can cause the brakes to overheat and lead to a fire. Unexpected continuous brake application can also cause the driver to lose control of the vehicle. Also, the brakes may be applied without illuminating the brake lights, failing to give proper warning to other drivers. Navistar will notify owners, and dealers will provide a temporary repair until Bendix develops a permanent remedy. The safety recall is expected to begin on or before April 6. Source: http://www-odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V052000&summary=true&prod_id=1170772&PrintVersion=YES

STIHL recalls chain saws due to risk of injury. The U.S. Consumer Product Safety Commission, in cooperation with STIHL Inc., February 14 announced a voluntary recall of about 3,000 STIHL MS 391 chain saws. Consumers should stop using recalled products immediately unless otherwise instructed. The flywheel on the chain saw can crack causing parts of the flywheel to separate and strike users or bystanders, posing a risk of injury. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12108.html

Fire control panels recalled by Bosch Security Systems Corp. due to alarm failure posing a fire hazard. The Consumer Product Safety Commission, in cooperation with Bosch Security Systems Corp., February 15 issued a recall of about 330 fire alarm control panels. Consumers should stop using the product immediately unless otherwise instructed. On all systems, when the alarm verification feature of the system is turned on, the control panel can fail to sound an alarm if a fire occurs. In addition, on systems with 50 or more reporting stations, a delay in sounding an alarm and reporting a fire may occur if the loop for the alarm system is broken. All distributors and installers are being sent two technical bulletins. One provides instructions for how to implement a software change that will correct the verification feature. The second contains instructions for how to handle warnings from affected systems with 50 or more stations. Those who have not received the bulletins should contact Bosch. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml12/12721.html

Defense/ Industry Base Sector

Problems with motor slow U.S. AMRAAM buys. The Pentagon slowed down its purchases of the new AIM-120D version of the Advanced Medium Range Air-to-Air Missile (AMRAAM) because of problems with producing its rocket motors, the U.S. Air Force's top acquisition official said February 14. "They're behind on the delivery of the missile," he said of the Raytheon-produced system. The Air Force reduced the number of missiles it is buying to 113 units, down from 138 the year before. Overall, the Pentagon plans to spend $423 million on continued production of the active radar-guided AIM-120D for a total of 180 missiles, including Navy and Marine Corps buys. The official said the quality of the missiles already delivered is

"fine," but the weapons cannot be produced in quantity due to a high rejection rate for the rocket motors being built. However, the Pentagon must have the new AMRAAM variant. The next-generation Joint Dual-Role Air Dominance Missile, which would have replaced the AMRAAM and the AGM-88 High Speed Anti-Radiation missile, which is used to suppress enemy air defenses, was terminated because it was unaffordable. Source: http://www.defensenews.com/article/20120214/DEFREG02/302140011/Problems-Motor-Slow-U-S-AMRAAM-Buys?odyssey=tab|topnews|text|FRONTPAGE

(Pennsylvania) **Anonymous movement claims hacking attack on U.S. tear gas company.** The Web site of a Jamestown, Pennsylvania-based company whose tear gas was used against demonstrators in Egypt is the latest to be broken into by the Anonymous movement, the hackers claimed February 14. In a statement posted to the Internet, the hackers accused Combined Systems of being war profiteers who sell "mad chemical weapons to militaries and cop shops around the world." Anonymous said it targeted Combined Systems because it was supplying weaponry used to "to repress our revolutionary movements." The hackers also claimed to have stolen and published personal information belonging to clients and employees of the firm. Allegedly intercepted e-mails were pasted onto the bottom of the statement; one of them appeared to be a warning that Combined Systems' site was sabotaged. Neither the hackers' claims nor the authenticity of the e-mails could be immediately verified, although the Web site was down February 14. The company sells a variety of security wares, including aerosol grenades, sprays, and handcuffs. Source: http://www.usatoday.com/tech/news/story/2012-02-14/anonymous-hacks-tear-gas/53087858/1

Emergency Services

(California) **FBI probes deadly shooting involving ICE agents in Long Beach.** About 100 FBI agents February 16 were combing a shooting scene in Long Beach, California, where a federal agent had wounded his supervisor before being fatally shot by another agent. The FBI agents were interviewing witnesses and processing the crime scene after the dispute between the agents with the federal Immigrations and Customs Enforcement agency, known as ICE, at the Glenn M. Anderson Federal Building. Multiple law enforcement authorities told the Los Angeles Times the shooting involved a dispute between an agent and his supervisor. The agent opened fire repeatedly on the male supervisor in the building, according to the sources. With the supervisor wounded, a third agent intervened and opened fire on the gunman, who was pronounced dead at the scene, according to law enforcement authorities. The supervisor was taken to a nearby hospital. The Long Beach Police Department, which initially responded to the call, was investigating the shooting with FBI. They were being aided by the ICE office of Professional Responsibility. Source: http://latimesblogs.latimes.com/lanow/2012/02/fbi-probes-ice-agent-shooting.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+lanowblog+(L.A.+Now)

(Florida) **2 Clay County deputies shot, 1 dies.** Two deputies were shot during a raid of a suspected meth lab in Middleburg, Florida, February 16. One of those deputies and a suspect shot as he ran from the scene both died, according to the Clay County sheriff. The second deputy was also hit by gunfire in the incident. The second detective was struck in the arm and was taken to a nearby medical center where he was listed in serious but stable condition. Five people were arrested at the scene, and authorities said at least some of them may have been staying at the house without the knowledge or permission of the owners. The Florida Department of Law Enforcement will be the lead agency in the investigation of the police-involved shooting and will also assist in the clean up of the drug lab. Source: http://www.news4jax.com/news/2-Clay-County-deputies-shot-1-dies/-/475880/8796158/-/jntoxo/-/index.html?hpt=ju_bn4

Energy

Gas well inspections to be required after fracking, U.S. Secretary of the Interior says. Natural-gas drillers will be required by U.S. rules to inspect their wells after hydraulic fracturing on public land to ensure the safety of drinking-water supplies, the Secretary of the Interior said February 14. In the coming weeks, the Department of the Interior will propose standards under which companies such as Chesapeake Energy Corp. and Exxon Mobil Corp. must disclose the chemicals in the mixture injected underground to free trapped gas, demonstrate the well is not leaking, and check the work after fracking. The agency will also require that drilling on federal land meets guidelines for handling fracking water that returns to the surface after being injected into the rock to make sure streams are not contaminated. Source: http://www.bloomberg.com/news/2012-02-14/gas-well-inspections-to-be-required-after-fracking-salazar-says.html

Food and Agriculture

Canada beef recall tied to E. coli illness. One person is ill and the Canadian Food Inspection Agency (CFIA) and New Food Classics are warning the public not to consume certain Country Morning Beef Burgers, and no name Club Pack Beef Steakettes, because the beef may be contaminated with E. coli O157:H7, Food Safety News reported February 23. The Country Morning Beef Burgers were distributed to COOP and TGP grocery stores in British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, North West Territories, Yukon Territories, and Nunavut. The no name Club Pack Beef Steakettes were distributed by Loblaws. Source: http://www.foodsafetynews.com/2012/02/canada-ground-beef-recall-tied-to-e-coli-illness/

CDC: Raw milk much more likely to cause illness. Raw milk and raw milk products are 150 times more likely than their pasteurized counterparts to sicken those who consume them, according to a 13-year review published by the Centers for Disease Control and Prevention (CDC) February 21. States that permit raw milk sales also have more than twice as many illness outbreaks as states where raw milk is not sold. The CDC study, published online in Emerging Infectious Diseases, reviewed dairy-related outbreaks between 1993 and 2006 in all 50 states, during which time the authors counted 121 outbreaks resulting in 4,413 illnesses, 239

hospitalizations, and 3 deaths. Despite raw milk products accounting for about1 percent of dairy production in the United States, raw milk dairies were linked to 60 percent of dairy-related outbreaks. In addition, 202 of the 239 hospitalizations (85 percent) resulted from raw milk outbreaks. Thirteen percent of patients from raw milk outbreaks were hospitalized, versus 1 percent of patients from pasteurized milk outbreaks. Currently, 30 states permit the sale of raw milk, while another 7 are considering raw milk legislation changes in 2012. Source: http://www.foodsafetynews.com/2012/02/cdc-raw-milk-much-more-likely-to-cause-illness/

Jimmy John's permanently dropping sprouts from menus. Jimmy John's Gourmet Sandwich franchise owners and customers were told the chain is permanently dropping sprouts from the menu, Food Safety News reported February 20. Jimmy John's restaurants are currently associated with a five-state outbreak of the rare O26 strain of E. coli. It is the fifth outbreak involving sprouts traced back to Jimmy John's since 2008. While there has been no public comment by Jimmy John's since the outbreak was announced February 15, a Kirkville, Missouri franchise owner said the chain's founder ordered all sprouts permanently removed from the menu. After a 2010 outbreak, the founder switched the sandwich chain to clover sprouts after Salmonella illnesses were associated with alfalfa sprouts. He thought clover sprout seeds were smoother and would be easier to clean. Jimmy John's is not alone among sandwich chains who have decided sprouts are too risky. The 230-unit Jason's Deli dropped sprouts for at least the balance of 2012 as a food safety concern. The current O26 outbreak prompted the Erbert and Gerbert's Sandwich Shops in seven states to drop sprouts. Source: http://www.foodsafetynews.com/2012/02/jimmy-johns-gourmet-sandwich-franchise/

65 Campylobacter infections now tied to raw milk dairy. An additional five cases have bumped up the number of confirmed Campylobacter infections linked to raw milk produced by the Your Family Cow dairy in Chambersburg, Pennsylvania, to 65, the Pennsylvania Department of Health reported February 13. The latest breakdown of illnesses by state are: Pennsylvania (56); Maryland (4), West Virginia (3) and New Jersey (2). Unpasteurized milk in two unopened bottles from the dairy tested positive for the outbreak strain, according to Maryland health officials. After making some improvements to its equipment, the Family Cow dairy was cleared by the Pennsylvania Department of Agriculture to resume selling raw milk the week of February 6. Source: http://www.foodsafetynews.com/2012/02/65-campylobacter-infections-now-tied-to-raw-milk-dairy/

Government Sector (including Schools and Universities)

Suspicious powder sent to more Senate offices. Several more U.S. Senate state offices received "threatening mail containing a suspicious powdery substance" though the messages were found to be harmless, the Senate Sergeant-at-Arms told CBS News February 23. The latest incidents follow a string of similar mailings to congressional offices outside Washington, D.C. and media organizations February 22 that also proved to be harmless, according to authorities. The Sergeant-at-Arms said "it is clear that the person sending these letters is organized and

committed, and the potential to do harm remains very real." Letters were also sent to several media organizations, including to some Comedy Central comedians. The author told the comedians he would send letters to all 100 senators and 10 percent of them would contain "lethal pathogens," an official told CBS News. The letters delivered February 22 were postmarked Portland, Oregon. The Portland return address on the letters appeared to be phony. Source: http://www.cbsnews.com/8301-250_162-57383520/suspicious-powder-sent-to-more-senate-offices/

Anonymous hacks Federal Trade Commission Web sites. Internet activist group Anonymous hacked two Web sites of the Federal Trade Commission (FTC) February 14 and posted a violent video satirizing the Anti-Counterfeiting Trade Agreement (ACTA). The hackers attacked the FTC's Bureau of Consumer Protection's Business Center and a site promoting the National Consumer Protection Week. The main FTC Web page was unaffected. "The FTC takes these malicious acts seriously," the FTC spokeswoman said in a statement. "The sites have been taken down and will be brought back up when we're satisfied that any vulnerability has been addressed." Both sites were inaccessible February 17. The hackers replaced the government Web sites with a German-language video depicting a man in a ski mask gunning down people for downloading copyrighted music. In a profanity-laced statement, Anonymous promised to "rain torrential hellfire down on all enemies of free speech, privacy and internet freedom" if ACTA is approved. Source: http://thehill.com/blogs/hillicon-valley/technology/211395-anonymous-hacks-federal-trade-commission-websites

(Washington D.C.) **Terror suspect arrested near Capitol in FBI sting.** Police said a terrorism suspect has been arrested in an FBI sting operation near the U.S. Capitol while planning to detonate what he thought were explosives in Washington, D.C. U.S. Capitol Police said their officers and FBI officials arrested the man February 17 in a sting operation. A Justice Department spokesman said the suspect was closely monitored by law enforcement, and the purported explosives were deactivated, so the public was not in danger. Two people briefed on the matter told the Associated Press he was not arrested on the Capitol grounds, and the FBI has had him under surveillance around the clock for several weeks. A U.S. law enforcement official said the person arrested was canvassing the U.S. Capitol with violent intentions. He was not believed to have any known connections to al Qai'da. It was not immediately clear whether he was a U.S. citizen. Source: http://www.ajc.com/news/nation-world/terror-suspect-arrested-near-1353002.html

Stratfor clients now targeted with malware. The customers of Stratfor, a U.S.-based research group that provides geopolitical analysis to government organizations and major corporations, are being targeted again with malicious spam e-mails. Following the December breach of the company's servers by Anonymous and the stealing of names, home addresses, credit card details, and passwords of its clients, those very clients began to receive spear-phishing e-mails purportedly being sent by Stratfor's CEO, asking them to fill out an attached document with personal information. This time, the e-mails appear to be sent by a Stratfor administrator, who first warns clients not to open e-mails and attachments from "doubtful senders," and then urges them to download (attached) security software to check their systems for a nonexistent

piece of malware. “The link displayed in the emails appears legitimate at first glance, but looking closely at the target address, you notice that it doesn’t originate from the address in the email text,” according to Microsoft. “Stratfor is based in Texas, United States however the download URL is located somewhere in Turkey. A sample of another PDF file contained a download link for yet another compromised site, this time in Poland.” Less careful users will end up with a malicious PDF file or a variant of the Zbot information stealer trojan on their systems. Source: http://www.net-security.org/malware_news.php?id=1996

(Utah) **Man charged in assassination plot of Utah governor.** A Utah man who police said threatened to assassinate the governor of Utah and conducted surveillance on the governor’s mansion is facing multiple felony charges, the Associated Press reported February 12. The suspect was charged February 10 in Salt Lake City with felony counts of drug and weapons possession, along with a misdemeanor count of threatening elected officials. The man sent text messages to a friend February 2 stating that he was in the bushes and intended to kill the governor, court records said. The recipient of the texts reported the messages to police, and the suspect was arrested the same day. The texts also included a threat to kill a police officer who had driven past the mansion more than once during the suspect’s period of surveillance. Police also said the governor was at home during the time the man was conducting surveillance and was removed from the premises for safety reasons. Investigators enlisted the help of the message recipient to get him to come to a nearby gas station, where he was arrested. Police found containers of ammunition, a large knife, explosives, illegal fireworks, and small plastic bags of methamphetamine in the suspect’s truck. Security camera video from the area around the mansion also showed him conducting his surveillance. Source: http://www.huffingtonpost.com/2012/02/13/gary-herbert-utah-governor-assassination-brian-biff-baker_n_1272870.html?1329141901&ncid=edlinkusaolp00000008

Anonymous reverse ferrets on CIA.gov takedown. Hacking collective Anonymous claimed responsibility for making the CIA’s Web site inaccessible February 10, but later said it was just reporting the event, The Register reported February 13. The apparent distributed denial of service attack against the agency’s Web presence follows a week after the release of a recording of a conference call between FBI and British law enforcement officials discussing the progress of various cases against alleged members of Anonymous and LulzSec. A Twitter account associated with the activists’ movement claimed credit for the takedown before backtracking and saying it was merely “noting” the cia.gov site was inaccessible. The conflicting statements created confusion about the cause of the outage. A CIA representative confirmed problems with the agency’s site without commenting on the reasons for the downtime. The site returned to normal operation February 11. The site (which essentially serves as an online brochure for the agency and an outlet for public relations material) has been the target of hacktivists in the past, including a June 2011 attack by LulzSec. Source: http://www.theregister.co.uk/2012/02/13/cia_website_outage/

Uzbek national pleads guilty to plotting to kill the U.S. President on terror charges. An Uzbek national pleaded guilty in federal court February 10 to trying to kill the U.S. President and to supporting an Uzbek terror group. The man, who has been in the United States since

overstaying a student visa in 2009, pleaded guilty to charges of threatening to kill the President, possession of an illegal weapon, and supporting the Islamic Movement of Uzbekistan, which is a U.S.-designated terror group. He was living in the Birmingham, Alabama, areas when he was indicted by a federal grand jury on the Presidential threat and terror charges in July 2011 after he tried to obtain an automatic weapon to kill the President in a federal undercover operation spurred by confidential informants. He faces maximum prison sentences of 15 years on the terrorism charge, 5 years on the charge of threatening the President, and 10 years on the charge of being an illegal alien in possession of a firearm. Each charge also carries a maximum fine of $250,000. Source:
http://www.gsnmagazine.com/node/25624?c=federal_agencies_legislative

Information Technology and Telecommunications

New Zeus/SpyEye makes bots function as C&C servers. The latest build of the Zeus/SpyEye malware shows a change that could hamper security researchers' ability to take down the botnets using it and to track the criminals behind them. According to Symantec researchers, a previous build already moved towards replacing the bot-to-command and control (C&C) system with peer-to-peer capabilities so the bots receive configuration files from other bots, and this new one has finalized the transition. "This means that every peer in the botnet can act as a C&C server, while none of them really are one," said the researchers. "Bots are now capable of downloading commands, configuration files, and executables from other bots — every compromised computer is capable of providing data to the other bots." Apart from making such a botnet practically immune to a takedown, the move also has the added benefit of making the tracking and blocking of IP addresses of the C&C servers obsolete. Source: http://www.net-security.org/malware_news.php?id=2009

TeamHav0k finds XSS in British, French, and US government sites. As Operation XSS, the operation launched by the grey hats from TeamHav0k, continues, the hackers managed to identify cross-site scripting vulnerabilities in the official Web sites of governments from all over the world. Those countries included the United Kingdom, France, Brazil, and the United States in a statement by TeamHav0k, Softpedia reported February 22. Besides their statement, the post also contains a proof-of-concept to show that the site of France's Ministry of Agriculture, Food, Fishing, Rural, and Regional Development contains a major XSS flaw that can be utilized by an attacker to take over an unsuspecting user's session. A similar vulnerability was identified on the official site dedicated by the French government to outdoor sports. The domains owned by the Newport City Council and the Marine Accident Investigation Branch from Great Britain are on the list of potential victims. Finally, the U.S. site noted as being insecure belongs to the California Department of Pesticide Regulation, the organization that is in charge of monitoring the use of pesticide and its effects on public safety. Source:
http://news.softpedia.com/news/TeamHav0k-Finds-XSS-in-British-French-and-US-Government-Sites-254306.shtml

Cutwail botnet resurrects, launches massive malware campaigns using HTML attachments. Security researchers from M86Security are contributing the increase in malicious malware

campaigns using HTML attachments to the resurrection of the Cutwail botnet, responsible for "spamvertising" these campaigns, ZDNet reported February 17. Using the company's sensor networks, the researchers observed three peaks of "spamvertised" malicious campaigns using HTML attachments for serving client-side exploits to unsuspecting users. The campaigns include the FDIC "Suspended bank account" spam campaign, the "End of August Statement" spam campaign, and the "Xerox Scan" spam campaign. Once the user downloads and views the malicious attachment, JavaScript will redirect her to the client-side exploiting URL part of the malicious network currently relying on the Phoenix Web malware kit. Once the researchers obtained access to the command and control interface of the exploit kit, they noticed the majority of referrers were coming from "blank" referrer, meaning these are end and corporate users downloading and viewing the malicious attachments on their computers. Source: http://www.zdnet.com/blog/security/cutwail-botnet-resurrects-launches-massive-malware-campaigns-using-html-attachments/10398

Cybercriminals building intricate, multiuse malnets. Cybercriminals have gotten so sophisticated that they can build an intricate network infrastructure and use it repeatedly for the distribution of malware, according to a new study from Blue Coat Systems. These malware networks, or malnets, lure targets through trusted Web sites, then route them to malware through relay, exploit, and payload servers to deliver the malware payload. While malnets are becoming increasingly sophisticated, Blue Coat said these assets can be identified and the malware attacks blocked. However, the Blue Coat Systems 2012 Security Report notes that these malnets are constantly on the move, making them hard to pin down. In one case, in early February, a malware payload changed locations more than 1,500 times in a single day. Source: http://www.networkcomputing.com/security/232600910

Android suddenly the top target as mobile malware rises sharply, study finds. The amount of malicious code written for mobile devices, such as smart phones and tablets, jumped by 155 percent in 2011 and has grown more sophisticated, according to a new report from Juniper Networks' Mobile Threat Center. The magnitude of the growth is surprising, said Juniper's vice president of government affairs and critical infrastructure protection. "It's a direct result of consumer demand." Spyware makes up the bulk of identified mobile malware, accounting for 63 percent. The SMS trojan accounts for 36 percent of mobile malware. The amount of malware written for Android increased exponentially in 2011, going from 400 identified samples in June to more than 13,000 in December. In 2010, more than 70 percent of identified malware was written for Java ME, with another 27 percent for Symbian. BlackBerry, Android, and Windows Mobile accounted for no more than"other." In 2011, Android was the top target, with nearly 47 percent of identified malware, and Java ME had dropped to a still respectable 41 percent. Symbian accounted for 11.5 percent. Source: http://gcn.com/Articles/2012/02/16/Mobile-malware-Android-top-target.aspx?Page=1

New powerful bot spreads by e-mail. PandaLabs reported the presence of a powerful new bot called Ainslot.L. This malware is designed to log user activities, download additional malware, and take control of users' systems. Additionally, it acts as a banker Trojan, stealing log-in information related to online banking and financial transactions. Ainslot.L also performs scans

on the computer to seek and remove other bots, becoming the only bot on one's system. "What makes this bot different is that it eliminates all competition, leaving the computer at its mercy," explained the technical director of PandaLabs. Ainslot.L spreads via a fake e-mail purporting to come from a UK clothing company called CULT. The message informs users that they have placed an order in the amount of 200 pounds on CULT's online store and the invoice amount will be charged to their credit card. The text includes a link to view the order which actually downloads the bot onto the computer. Source: http://www.net-security.org/malware_news.php?id=2001

Fake Facebook notification delivers keylogger. Fake Facebook notifications about changes in users' account information have been hitting inboxes and delivering malware to unwary users, warn Barracuda Labs researchers. The e-mail address of the sender is spoofed to make it look like it has been sent by the social network, and the message contains only an image implying that the recipient needs to install Silverlight in order to view the content. Hovering with mouse over the image shows that the offered file is a Windows PIF file, and that is hosted on an IP address in Malaysia. The file is actually a keylogger, the Jorik Trojan. Once the keylogger is installed, it starts recording every keystroke and Web page title into a disk file, which is ultimately sent to a C&C server operated by cyber criminals. Source: http://www.net-security.org/malware_news.php?id=2002

Cyber criminals find new way to exploit old Office hole. Cyberattackers found a new way to take advantage of an old Microsoft Office hole. Symantec researchers noticed a specially crafted trojan that exploits a previously patched vulnerability. The attack occurs when a user opens up an e-mail that contains a Microsoft Word file with a malicious Dynamic Link Library file (DLL). "The exploit makes use of an ActiveX control embedded in a Word document file," a researcher at Symantec said. "When the Word document is opened, the ActiveX control calls fputlsat.dll which has the identical file name as the legitimate .dll file used for the Microsoft Office FrontPage Client Utility Library." He said once this flaw is exploited, an attacker is free to load up an infected system with malware. He also advises that if a user sees an e-mail attachment with the file name ftutlsat.dll, proceed with caution. An e-mail with this type of attachment should be easy to spot, according to the researcher. The exploit, recently seen in the wild by the security firm, was previously fixed by Microsoft in September's Security Update, bulletin MS11-073. The researcher warns that because the bulletin was only classified as "important" by Microsoft, it might have been overlooked. Source: http://gcn.com/articles/2012/02/10/trojan-exploits-unpatched-office-vulnerability.aspx

Waledac Botnet returns, steals passwords and credentials. In 2010, Microsoft was able to terminate the activity of the Waledac botnet, which at the time was famous for being a large source of spam. However, Palo Alto Networks researchers came across a new variant which is not only used for spamming, but also for stealing sensitive data from infected devices. The new version was spotted February 2. Experts conclude it is still sending spam, but it can also steal passwords and authentication data, including credentials for FTP, POP3, SMTP. Besides this, Waledac also steals .dat files for FTP and BitCoin and uploads them to the botnet. By relying on their WildFire systems, which enable a firewall to capture unknown files and analyze them in a

malware sandbox, Palo Alto Networks was able to identify how the new variant behaves. Given the confusion created around the Kelihos botnet that was declared resurrected by Kaspersky, only to be put to sleep again by Microsoft, the company emphasizes this is not the old botnet, but a new variant. Source: http://news.softpedia.com/news/Waledac-Botnet-Returns-Steals-Passwords-and-Credentials-253071.shtml

Researchers crack online encryption system. An online encryption method widely used to protect banking, e-mail, e-commerce, and other sensitive Internet transactions is not as secure as assumed, according to a report issued by a team of U.S and European cryptanalysts. The researchers reviewed millions of public keys used by Web sites to encrypt online transactions and found a small but significant number to be vulnerable. In most cases, the problem had to do with the manner in which the keys were generated, according to the researchers. The numbers associated with the keys were not always as random as needed, the research showed. Therefore, the team concluded, attackers could use public keys to guess the corresponding private keys that are used to decrypt data — a scenario previously believed to be impossible. Source: http://www.computerworld.com/s/article/9224265/Researchers_crack_online_encryption_system?taxonomyId=17

Horde FTP server hacked, files maliciously altered. The developers of the popular open source Web mail solution Horde identified a number of manipulated files on an FTP server. They concluded the server was breached, the files stored on it being altered to allow unauthenticated remote PHP execution. “We have immediately taken down all distribution servers to further analyze the extent of this incident, and we have worked closely with various Linux distributions to coordinate our response,” Horde officials said. After the investigation was concluded, the servers were replaced and secured, and the altered files replaced with clean variants. The analysis found three files were manipulated and modified on different occasions, and served to unsuspecting customers for about 3 months. Horde 3.3.12 was manipulated November 15, 2011, Horde Groupware 1.2.10 November 9, 2011, and Horde Groupware Webmail Edition 1.2.10 November 2, 2011. Since the incident was found February 7, users who downloaded the files during this timeframe are advised to immediately reinstall using fresh copies from Horde’s FTP server, or upgrade to more recent versions that have been released since. Horde 4 releases were not affected and neither were the company’s CVSs and Git repositories. The affected Linux distributions will provide notifications and security updates of their own. Users who are uncertain if they are exposed to cybercriminal operations can manually verify whether or not their products were altered by searching for the $m[1]($m[2]) signature in the Horde directory tree. Source: http://news.softpedia.com/news/Horde-FTP-Server-Hacked-Files-Maliciously-Altered-252708.shtml

Twitter turns on HTTPS by default. Twitter recently turned HTTPS on by default for all users. The option to always use HTTPS was made available to users in March 2011, but they had to turn it on for themselves by changing their account settings. Twitter’s very nature and the fact that many users are used to tweeting from unsecured Internet connections meant anyone

equipped with the Firesheep Firefox add-on can easily steal their log-in credentials sent via unencrypted HTTP sessions. Source: http://www.net-security.org/secworld.php?id=12396

National Monuments and Icons

Southern Utah cabin burglar considered armed and dangerous. A mountain recluse authorities said was responsible for more than two dozen cabin burglaries in the remote southern Utah wilderness near Zion National Park is considered armed and dangerous by authorities, KCSG 14 St. George reported February 21. Authorities identified him from fingerprints lifted from vacation homes near Zion National Park, which spans hundres of miles in Washington, Kane and Iron counties. The man remains somewhere in roughly 1,000 square miles of wilderness. He now faces multiple counts of burglary and a weapons charge. In a statement, the Iron County Sheriff's Office said tips from the public and forensic evidence linked the man to the crimes. "This suspect is known to be armed and could be possibly dangerous if cornered," the statement read. Source: http://www.kcsg.com/view/full_story/17617653/article-Southern-Utah-Cabin-Burglar-Considered-Armed-And-Dangerous?instance=home_stories8_tip

Postal and Shipping

(Delaware) **Del. post office evacuated because of suspicious package; 1 taken to hospital.** A suspicious package in Wilmington, Delaware, led to the evacuation of a post office and another building, and some roads were closed February 17. New Castle County paramedics told the News Journal of Wilmington that one person was taken to a hospital and several others were treated at the scene. Source: http://www.therepublic.com/view/story/266a12bd88a2416cad9b862d7603e361/DE--Suspicious-Package/

Public Health

FDA steps in to avert children's cancer drug shortage. The U.S. Food and Drug Administration (FDA) has stepped in to help avert an imminent shortage of methotrexate, a drug used to treat childhood blood cancer, after the main supplier of the drug, Bedford Laboratories' Ben Venue factory in Ohio, shut down the fall of 2011 because of production problems. In a statement an FDA spokeswoman sent via e-mail February 16: Bedford advised the FDA that it will release emergency supplies of preservative-free methotrexate to meet patient needs. This additional quantity of medicine was produced before the company voluntarily shut down and the company has worked to ensure that the drug was not impacted by the issues that led to the plant shutdown. Based on the information provided by the firms, the new supplies are anticipated to be available by the end of this month with ongoing releases in March. USA Today reported that the FDA is also working to secure foreign supplies. Source: http://commonhealth.wbur.org/2012/02/breaking-fda-steps-in-to-fix-childrens-cancer-drug-shortage/

Roche warns of counterfeit Avastin in U.S. The maker of the best-selling anticancer drug Avastin is warning doctors and patients about counterfeit vials of the product distributed in the United States, the Associated Press reported February 14. Roche's Genentech unit said the fake products do not contain the key ingredient in Avastin, which is used to treat cancers of the colon, lung, kidney, and brain. The company believes drugs labeled with the following lot numbers may be fake: B86017, B6011, and B6010. The counterfeit products do not have "Genentech" printed on their packaging, which appears on all FDA-approved cartons and vials. A spokeswoman said the counterfeit drug was distributed to health care facilities in the United States. The company is working with the Food and Drug Administration to track down the counterfeit vials and analyze their contents. It said it was alerted to the problem by foreign health regulators and believes the counterfeits were imported from abroad. Additionally, legitimate Avastin contains a six-digit lot number with no letters. All the text on the product's packaging is in English. Source: http://yourlife.usatoday.com/health/story/2012-02-14/Roche-warns-of-counterfeit-Avastin-in-US/53096312/1

FDA investigating illegal online sale of handheld dental x-ray units. The U.S Food and Drug Administration (FDA) is warning dental and veterinary professionals to not purchase or use certain potentially unsafe hand-held dental X-ray units. The FDA is concerned these devices may not be safe or effective, and could expose the user and the patient to unnecessary and potentially harmful X-rays. The units, sold online by manufacturers outside the United States and directly shipped to U.S. customers, have not been reviewed by the FDA and do not meet FDA radiation safety requirements. The Washington State Department of Health alerted the FDA after tests on a device purchased online revealed it did not comply with X-ray performance standards. All X-ray units that have been cleared by the FDA bear a permanent certification label/tag, a warning label, and an identification label/tag on the unit. Source: http://www.prnewswire.com/news-releases/fda-investigating-illegal-online-sale-of-handheld-dental-x-ray-units-139093199.html

Transportation

Nothing Significant to Report

Water and Dams

U.S. water shortages loom. More than one in three counties in the United States could face a "high" or "extreme" risk of water shortages due to climate change by the middle of the twenty-first century, according to a new study in the American Chemical Society's (ACS) journal Environmental Science & Technology. Homeland Security Newswire said February 24, the new report concluded 7 in 10 of the more than 3,100 U.S. counties could face "some" risk of shortages of fresh water for drinking, farming, and other uses. An American Chemical Society release reports that population growth is expected to increase the demand for water for municipal use and for electricity generation beyond existing levels. Global climate change threatens to reduce water supplies due to decreased rainfall and other factors compared to levels in the twentieth century. The group developed a "water supply sustainability risk index"

that takes into account water withdrawal, projected growth, susceptibility to drought, projected climate change, and other factors in individual U.S. counties for the year 2050. It takes into account renewable water supply through precipitation using the most recent downscaled climate change projections and estimates future withdrawals for various human uses. The team used the index to conclude climate change could foster an "extreme" risk of water shortages that may develop in 412 counties in southern and southwestern states and in southern Great Plains states. Source: http://www.homelandsecuritynewswire.com/dr20120224-u-s-water-shortages-loom

Nationwide radium testing of groundwater shows most susceptible regions are central U.S. and East Coast. According to a study conducted by the U.S. Geological Survey (USGS), groundwater in aquifers on the East Coast and in the central United States have the highest risk of contamination from radium, a naturally occurring radioactive element and known carcinogen. Radium was detected in concentrations that equaled or exceeded U.S. Environmental Protection Agency (EPA) drinking water standards in more than one in five wells tested in the Mid-Continent and Ozark Plateau Cambro-Ordovician aquifer systems, underlying parts of Arkansas, Illinois, Indiana, Iowa, Michigan, Minnesota, Missouri, and Wisconsin; and the North Atlantic Coastal Plain aquifer system, underlying parts of Delaware, Maryland, New Jersey, New York, North Carolina, and Virginia. The study found that if the groundwater has low oxygen or low pH, radium is more likely to dissolve and become present. Low oxygen conditions were prevalent in the Mid-Continent and Ozark Plateau Cambro-Ordovician aquifer systems, and low pH conditions were prevalent in the North Atlantic Coastal Plain aquifer system. In most aquifers used for drinking water, radium concentrations were below EPA standards, especially in the West. Source: http://www.usgs.gov/newsroom/article.asp?ID=3104

(Ohio) **EPA begins testing sites for contamination.** The U.S. Environmental Protection Agency (EPA) began testing 14 sites in Sandusky County, Ohio, February 13 for possible contamination, a study spurred by a high number of childhood cancer cases in the area. Since the mid-1990s, at least 35 children in a 12-mile radius in the east half of the county have been diagnosed with various types of cancer. Four have died. The study may not find the root cause of the cluster, but any contamination it does uncover would still help the community, said the county administrator whose 11-year daughter, died of cancer in 2009. The sites, many of which are former dumps, were determined as possible areas of contamination by a 2009 study of the cancer cluster. Crews will take soil, water and gas samples from the ground at each site, a process expected to take 2-3 weeks. After the samples are tested and analyzed, the EPA expects to report any findings in the late spring or early summer. Source: http://www.thenews-messenger.com/article/20120213/NEWS01/120213007/EPA-begins-testing-sites-contamination

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168